

**IN THE UNITED STATES DISTRICT COURT FOR THE MIDDLE  
DISTRICT OF PENNSYLVANIA**

<b>JOAN LONGENECKER-WELLS,</b>	:	
<b>KENNETH DODSON,</b>	:	
<b>GENEVIEVE REGAL, BENJAMIN</b>	:	CIVIL ACTION
<b>HUFFNAGLE, and NICHOLAS</b>	:	HON. WILLIAM W. CALDWELL
<b>DANKOSKY, individually and on</b>	:	NO. 1:15-CV-00422-WWC
<b>behalf of all others similarly situated,</b>	:	
	:	
<b>Plaintiffs</b>	:	<b>CLASS ACTION</b>
	:	<b>COMPLAINT</b>
<b>v.</b>	:	
	:	
<b>BENECARD SERVICES, INC.</b>	:	
<b>d/b/a BENECARD PBF,</b>	:	
<b>BENECARD CENTRAL FILL</b>	:	
<b>OF PA, LLC, BENECARD</b>	:	
<b>MARKETING, L.L.C., NATIONAL</b>	:	JURY TRIAL DEMANDED
<b>VISION ADMINISTRATORS</b>	:	
<b>LLC, and CONTACT FILL, LLC</b>	:	
	:	
<b>Defendants</b>	:	

**AMENDED CLASS ACTION COMPLAINT**

AND NOW, come the Plaintiffs, Joan Longenecker-Wells, Kenneth Dodson, Genevieve Regal, Benjamin Huffnagle, and Nicholas Dankosky (collectively the "Plaintiffs"), through counsel, individually and on behalf of all others similarly situated (the proposed "Class"), who bring this Amended Class Action Complaint against Benecard Services, Inc. d/b/a Benecard PBF, Benecard Central Fill of PA,

LLC, Benecard Marketing, L.L.C., National Vision Administrators LLC, and Contact Fill, LLC (collectively the “Defendants” or "Benecard"), and aver the following:

### **NATURE OF THE ACTION**

1. The Plaintiffs bring this Class Action Complaint on behalf of themselves and all other current and former employees and customer members of the Defendants whose private information (the “Information”) was wrongfully disclosed to unknown persons (the “Security Breach” or “Breach”).
2. The Defendants had a duty to protect and adequately secure this Information, which was highly confidential.
3. The Defendants violated this duty, resulting in the aforementioned Security Breach, and this Breach resulted in significant injury to the Plaintiffs and proposed Class members, which is described in detail herein.
4. In addition, the Defendants failed to adequately and timely notify the Plaintiffs and proposed Class members of the Security Breach, causing further irreparable financial injury.

### **JURISDICTIONAL STATEMENT**

5. This Court has original jurisdiction over this action under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2). The amount in controversy in this action exceeds \$5,000,000, exclusive of interests and costs,

there are more than 100 members of the proposed Class, as defined herein, and the Plaintiffs and proposed Class members are citizens of different states than one or more defendants.

6. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b), since Defendants regularly transact business in this District, and a substantial part of the events giving rise to this Complaint arose in this District.

## PARTIES

7. Plaintiff Joan Longenecker-Wells is a former employee and customer member of Benecard, residing in Pennsylvania.

8. Plaintiff Kenneth Dodson is a former employee and customer member of Benecard, residing in Pennsylvania.

9. Plaintiff Genevieve Regal is a former employee and customer member of Benecard, residing in Pennsylvania.

10. Plaintiff Benjamin Huffnagle is a former employee and customer member of Benecard, residing in Pennsylvania.

11. Plaintiff Nicholas Dankosky is a former employee and customer member of Benecard, residing in Pennsylvania.

12. Defendant Benecard Services, Inc. (“Benecard”) is a New Jersey corporation and Pennsylvania Foreign Corporation with a registered address in

Dauphin County, Pennsylvania, which does business under the Pennsylvania registered fictitious name of Benecard PBF.

13. Defendant Benecard Central Fill of PA, LLC (“Benecard Central”) is a Florida corporation and Pennsylvania Foreign Limited Liability Company with a registered address in Dauphin County, Pennsylvania.

14. Defendant Benecard Marketing, L.L.C. (“Benecard Marketing”) is a New Jersey corporation and Pennsylvania Foreign Limited Liability Company with a registered address in Dauphin County, Pennsylvania.

15. Defendant National Vision Administrators LLC (“National Vision”) is a New Jersey corporation and Pennsylvania Foreign Limited Liability Company with a registered address in Dauphin County, Pennsylvania.

16. Defendant Contact Fill, LLC (“Contact Fill”) is a Pennsylvania Domestic Limited Liability Company with a registered address in Dauphin County, Pennsylvania.

17. Benecard’s family of companies includes Benecard PBF, Benecard Central, Benecard Marketing, National Vision, and Contact Fill, all of which are believed to be subsidiaries of the Ullman Family Partnership, LP, which is a New Jersey partnership and Pennsylvania Foreign Limited Partnership with a registered address in Dauphin County, Pennsylvania.

18. Benecard and its family of companies provide prescription benefit administration services that include mail and specialty drug dispensing, managed vision services, and contact lens mail service to private and public sector organizations with 100 to 5,000+ members. Benecard has offices in New Jersey, Pennsylvania, and Florida.

**DEFENDANTS' NOTICE OF POTENTIAL SECURITY BREACH AND FINANCIAL HARM TO EMPLOYEES AND CUSTOMER MEMBERS**

19. The Defendants had actual and significant notice of the risk of a security breach and the resultant financial harm posed to the Plaintiffs and proposed Class members.

20. In fact, in September 2011, Benecard suffered a prior security breach that affected current employees and customer members.

21. After the prior September 2011 breach, several affected current employees and customer members had fraudulent tax returns filed in their names.

22. In addition to the aforementioned prior security breach, the Defendants had further notice of the risk of a Security Breach and the resultant financial harm posed to the Plaintiffs and proposed Class members, as such risks are commonly understood and companies like Defendants are routinely warned about such Breaches.

23. For example, the 2013 Identity Fraud Report released by Javelin Strategy & Research ("Javelin Report") reported that in 2012 identity fraud

incidents increased by more than one million victims, and fraudsters stole nearly \$21 billion.

24. The 2013 Javelin report found 12.6 million victims of identity fraud in the United States in the last year, equating to 1 victim every 3 seconds.

25. The 2013 Javelin report also found that nearly one in four data breach letter recipients become a victim of identity fraud, with breaches involving Social Security numbers to be the most damaging.

26. More recently, Javelin Strategy & Research released its 2014 report, which further highlighted the continued danger from security breaches.

27. The 2014 Javelin report found that 13.1 million people fell victim to identity fraud, over 1 million more than in 2013.

28. The United States Government has also warned companies to carefully protect their employees' and customer members' sensitive private information.

29. To assist companies in protecting the security of such information, the Federal Trade Commission ("FTC") has issued a publication entitled "Protecting Personal Information: A Guide for Business" (the "FTC Guide").

30. The FTC Guide advises companies to "pay particular attention to how you keep personally identifying information: Social Security numbers, credit card

or financial information, and other sensitive data. That's what thieves use most often to commit fraud or identity theft."

31. The FTC Guide further advises companies regarding basic protocols that should be followed to protect such sensitive information, including how to secure the information and respond to security incidents.

### **THE ACTUAL SECURITY BREACH AND RESULTANT DAMAGE**

32. Prior to commencing employment with the Defendants and/or using the Defendants' services as customer members, the Plaintiffs and proposed Class members provided the Defendants with private Information, including, but not limited to, their full names, dates of birth, addresses, and social security numbers.

33. The Plaintiffs and proposed Class members providing this information to the Defendants was a prerequisite to employment with the Defendants, and/or utilizing the Defendants' services.

34. Throughout the course of the Plaintiffs' and proposed Class members' employment and/or customer member relationship, the Defendants maintained the Plaintiffs' and proposed Class members' confidential personal financial information, including, but not limited to, W-2 tax forms.

35. The Plaintiffs and proposed Class members reasonably expected that the Defendants would protect this information from a breach.

36. The Plaintiffs and proposed Class members would not have provided their confidential personal financial information to the Defendants had they known that the Defendants would not adequately protect such information.

37. The Plaintiffs' and proposed Class members' Information, which was held and secured by the Defendants was compromised and/or otherwise misappropriated by unknown parties within the past several months.

38. The Plaintiffs' and proposed Class members' Information was obtained by unknown parties due to the Defendants' failure to adequately protect and secure that Information.

39. The Defendants violated administrative guidelines, best practices, and industry standards regarding the security of the Plaintiffs' and proposed Class members' Information, and otherwise failed to adopt necessary policies and procedures to protect the release of the Plaintiffs' and proposed Class members' Information to unknown parties.

40. These oversights included, but were not limited to:

- a) failing to adequately encrypt confidential Information;
- b) failing to safely transmit confidential Information;
- c) failing to establish adequate firewalls to protect confidential Information;
- d) failing to protect from server intrusion;

e) failing to timely and appropriately handle, store, and destroy confidential Information; and,

f) failing to adequately protect confidential Information on their internal network.

41. The aforementioned violations and failures were the direct and proximate cause of the Plaintiffs' and proposed Class members' injuries.

42. Because of the Breach, unknown persons filed fraudulent tax returns in the Plaintiffs' and proposed Class members' names for the 2014 tax year, causing immediate and future financial injury.

43. It is believed, and therefore averred, that the IRS issued tax refunds to these unknown parties rather than to the Plaintiffs and proposed Class members.

44. The Plaintiffs and proposed Class members have also incurred additional financial harm, including, but not limited to, additional filing fees, accounting costs, and identity theft protection.

45. In addition to the filing of the fraudulent tax returns, the Defendants' failures enabled unknown parties to have access to the Information, which will likely be used to perpetrate further financial fraud.

46. The Plaintiffs and proposed Class members are now spending countless hours frantically attempting to perform damage control to prevent further devastation to their credit and livelihood.

47. The Defendants' failure to timely disclose the extent of the Security Breach and to notify those affected in a judicious manner has caused further damage to the Plaintiffs and the proposed Class members.

48. Defendants have failed to offer any explanation for the cause of the breach, how the unknown parties were able to access the Plaintiffs' and proposed Class members' Information, and what steps, if any, the Defendants have taken or will take in the future to ensure that the Information will be adequately protected.

### **NOTICE OF THE ACTUAL SECURITY BREACH**

49. It is believed, and therefore averred, that the Defendants learned that unknown persons obtained the Plaintiffs' and proposed Class members' Information on or about February 13, 2015.

50. On February 20, 2015, the Plaintiffs and proposed Class members then **presently employed** by the Defendants received an email notification from the Defendants stating that there “**may** have been unauthorized access to employee information.” (emphasis added).

51. The Defendants’ February 20, 2015 email notification further advised that due to this Breach “some employees have run into problems filing their 2014 tax returns.”

52. The Defendants’ February 20, 2015 email notification fails to clearly state that the Information had absolutely been misappropriated and was being used

by unknown parties to file fraudulent tax returns, although Defendants were well aware of this fact at the time of the notification.

53. Worse still, the Defendants' February 20, 2015 email notification was not sent to the Plaintiffs and proposed Class members who were then **former employees or customer members** of the Defendants.

54. On February 25, 2015, a second email notification was sent by the Defendants to the Plaintiffs and proposed Class members **presently employed** by the Defendants, which again advised "we have learned that fraudulent federal tax returns have been filed for some of our employees."

55. Again, this second email notification was not sent to the Plaintiffs and proposed Class members who were then **former employees or customer members** of the Defendants.

56. As of the original date of filing of the Class Action Complaint, the Plaintiffs and proposed Class members who were **former employees or customer members** of the Defendants had not received any notification of the Security Breach from the Defendants.

57. As of the original date of filing of the Class Action Complaint, none of the Plaintiffs and proposed Class members who are or used to be customer members of the Defendants or who work or used to work for the Defendants had

received information regarding the scope of the breach, or how many fraudulent tax returns had been filed.

58. Under Pennsylvania's Breach of Personal Information Notification Act, 73 Pa. Stat. § 2301 et seq., the Defendants had an obligation to provide notice of any breach without unreasonable delay, which Defendants failed to do.

### **CLASS ACTION ALLEGATIONS**

59. The Plaintiffs bring this action on their behalf and on behalf of all similarly situated persons as a Class Action pursuant to Federal Rule of Civil Procedure 23.

60. The Plaintiffs bring this action on behalf of two proposed Classes, to be defined as:

a) All current and former employees of the Defendants who are citizens of the United States whose personal and financial information was compromised and/or otherwise misappropriated.

b) All current and former customer members of the Defendants who are citizens of the United States whose personal and financial information was compromised and/or otherwise misappropriated.

61. The Plaintiffs are members of the Classes they seek to represent.

62. The Classes are so numerous that joinder of all members is impracticable, since (1) as many as 600 current and former employees' Information has been compromised, and (2) as many as 35,000 customer members' Information

has been compromised (referred to collectively as the "proposed Class" throughout this Complaint).

63. The members of the Classes are readily ascertainable, as they can be identified by records maintained by Defendants. Notice can be provided by means permissible under Rule 23.

64. The Plaintiffs' claims are typical of the claims of all the members of the Classes.

65. The Plaintiffs' and Class members' claims arise from the Defendants' failure to provide reasonable security measures and policies to protect their Information, which resulted in damages.

66. The conduct of the Defendants has caused actual injury and imminent threat of injury to the Plaintiffs and members of the Class.

67. Prosecuting separate actions by individual Class members would create a risk of inconsistent or varying adjudications.

68. The Plaintiffs will fairly and adequately represent the interests of the Class, as the named Plaintiffs have no interests antagonistic to or in conflict with those of the Class members.

69. The Plaintiffs are represented by experienced counsel, who are qualified to litigate this case.

70. A Class Action is superior to all other available methods for the fair and efficient adjudications of this controversy. Individual Class members' claims may be too small to justify the time and expense of litigation, which would render it impossible for them to address the Defendants' conduct. Permitting the Plaintiffs' and Class members' claims to proceed as a Class Action will advance the orderly resolution of this case, and promote judicial economy.

71. There are questions of law and fact common to all members of the Class, which predominate over individualized questions, including:

- a) Whether the Defendants provided adequate security and/or protection for the Plaintiffs' and proposed Class members' Information;
- b) Whether the Defendants' conduct resulted in the unauthorized access to the Plaintiffs' and proposed Class members' Information;
- c) Whether the Plaintiffs and proposed Class members are entitled to damages, and the measure of such damages.

**COUNT I**

**NEGLIGENCE**

72. The allegations throughout this Complaint are incorporated as if set forth at length.

73. The Defendants had a duty to exercise reasonable care to protect and secure the Plaintiffs' and the proposed Class members' Information from being

compromised, lost, stolen, misused, and/or otherwise disclosed to unauthorized parties.

74. The Defendants' duties included, but were not limited to, designing, implementing, maintaining, and testing security systems that ensured the Plaintiffs' and the proposed Class members' Information was adequately secured and protected, and that would detect a Security Breach in a timely manner.

75. Through the Defendants' acts and/or omissions, the Defendants breached their duties regarding the Plaintiffs' and proposed Class members' Information by:

- a) Failing to adequately monitor and provide for the security of the Information;
- b) Allowing unauthorized access to Plaintiffs' and the proposed Class members' Information;
- c) Failing to recognize in a timely manner that Plaintiffs' and proposed Class members' Information had been compromised.
- d) Failing to comply with industry standards relating to Information security; and,
- e) Unreasonably delaying informing the Plaintiffs and proposed Class members of the Security Breach.

76. Without the Defendants' negligent actions and/or omissions and breach of their duties owed to the Plaintiffs and proposed Class members, the Security Breach would not have occurred and the Plaintiffs' and proposed Class members' Information would not have been compromised and/or otherwise misappropriated.

77. The Plaintiffs' and proposed Class members' injuries were the reasonably foreseeable result of the Defendants' failure to exercise reasonable care in safeguarding, protecting, and/or securing the Plaintiffs' and proposed Class members' Information, as the Information provided by the Plaintiffs and proposed Class members is frequently the target of data breach crimes.

78. The Plaintiffs and proposed Class members are part of a well-defined and foreseeable class who were well known and identifiable to the Defendants.

79. The Defendants' negligent handling of the Information was the direct and proximate cause of the Plaintiffs' and proposed Class members' foreseeable harm.

80. As a result of Defendants' negligence, the Plaintiffs and proposed Class members have suffered actual damages including, but not limited to, lost 2014 tax refunds, expenses for re-filing, expenses for credit monitoring, identity theft protection, lost work time, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm.

81. In addition, as a result of the Defendants' negligence, the Plaintiffs and proposed Class members are at an increased and imminent risk of becoming victims of identity theft crimes, fraud and abuse.

## COUNT II

### BREACH OF IMPLIED CONTRACT

82. The allegations throughout this Complaint are incorporated as if set forth at length.

83. When the Defendants required the Plaintiffs and proposed Class members to supply their Information, the Defendants entered into an implied contract with the Plaintiffs and proposed Class members that the Defendants would protect the Information.

84. This implied contract arose from the course of conduct between the Plaintiffs and proposed Class members and the Defendants.

85. This implied contract required the Defendants to safeguard and protect the Plaintiffs' and proposed Class members' Information from being compromised and/or otherwise misappropriated.

86. The Defendants did not adequately safeguard or protect the Plaintiffs' and proposed Class members' Information from being compromised and/or otherwise misappropriated.

87. The Defendants did not adequately maintain sufficient security measures and procedures to prevent the unauthorized access to Plaintiffs' and proposed Class members' Information.

88. Because the Defendants failed to safeguard and/or protect the Plaintiffs' and proposed Class members' Information from being compromised and/or otherwise misappropriated, the Defendants breached the implied contract with the Plaintiffs and proposed Class members.

89. The Plaintiffs and proposed Class members have suffered and will continue to suffer damages as the result of the Defendants' breach, as described herein.

### **PRAYER FOR RELIEF**

WHEREFORE, the Plaintiffs, individually and on behalf of all others similarly situated, request this Court enter judgment against the Defendants in favor of the Plaintiffs and proposed Class members, and award the following:

- a) That this action be certified as a Class Action pursuant to Federal Rule of Civil Procedure 23;
- b) That Plaintiffs be declared as representatives of the Class, and Plaintiffs' counsel as counsel for the class;
- c) Award damages in excess of \$5,000,000; and,
- d) Award reasonable counsel fees and expenses.

Respectfully Submitted,

**ANDREOZZI & ASSOCIATES, P.C.**

Dated: June 23, 2015

/s/ Benjamin D. Andreozzi  
Benjamin D. Andreozzi, Esq.  
PA ID #89271  
ben@victimscivilattorneys.com

/s/ Nathaniel L. Foote  
Nathaniel L. Foote, Esq.  
PA ID #318998  
nate@victimscivilattorneys.com

111 N. Front Street  
Harrisburg, PA 17101  
717.525.9124 (Phone)  
717.525.9143 (Fax)  
*Attorneys for Plaintiffs*

**CERTIFICATE OF SERVICE**

I, Benjamin D. Andreozzi, Esq., counsel for Plaintiffs, hereby certify that a true and correct copy of the foregoing document was served upon the following counsel via this Court's electronic filing system.

David Shannon, Esq.  
djshannon@mdwcg.com

Lauren Burnette, Esq.  
lmburnette@mdwcg.com

Dated: June 23, 2015

/s/ Benjamin D. Andreozzi  
Benjamin D. Andreozzi, Esq.  
PA ID #89271  
ben@victimscivilattorneys.com